Краевое государственное бюджетное профессиональное образовательное учреждение
Хабаровский техникум транспортных технологий
имени Героя Советского Союза А.С. Панова

Безопасность в сфере осуществления финансовых операций онлайн

Введение

Цель работы – исследование вопроса безопасности в сфере электронных платежей, и пути защиты электронных денег.

Задачи:

1. Рассмотреть сущность и виды электронных денег.
2. Выявить риски потери электронных денег.
3. Рассмотреть виды финансового мошенничества
4. Создать рекомендации по вопросу защиты электронных денег.

- **Электронные деньги** - это денежные обязательства эмитента в электронном виде, которые находятся на электронном носителе в распоряжении пользователя.
- соответствуют следующим трем критериям:

1. *Фиксируются и хранятся на электронном носителе;*
2. *Выпускаются эмитентом при получении от иных лиц денежных средств в объёме не меньшем, чем эмитированная денежная стоимость;*
3. *Принимаются, как средство платежа другими (помимо эмитента) организациями.*

КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ ЭКО-СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

1. **Банк(и)** – эмитент электронных денег, гарант обеспечения электронных денег;
2. **Платежная Система(системы)** – обеспечивает технологические процессы эмиссии и развитие бизнес процессов;
3. **Бизнес среда** – используются и циркулируют электронные деньги – продукт совместной деятельности банка, платежной системы, торговцев и сервис провайдеров;

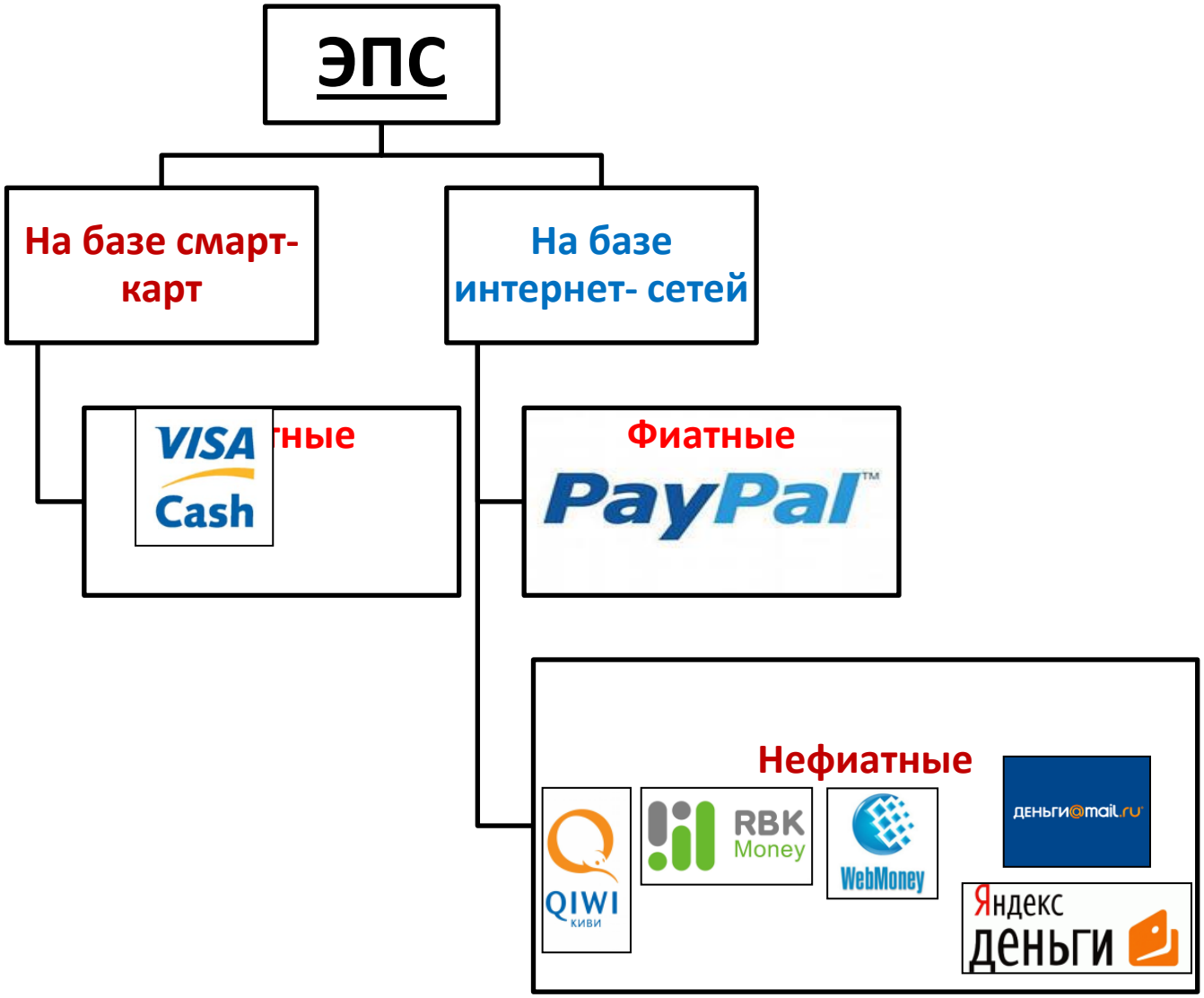
ГДЕ КУПИТЬ ДЕНЬГИ? (ВВОД СРЕДСТВ В СИСТЕМУ)

- **Интернет**
  - Веб-витрины
  - Обменные пункты
  - Сайт банка или системы
- **Клиент-банк**
  - Заказ и оплата из личного кабинета
- **Банкомат**
  - Банки партнеры
- **Терминалы**
  - POS терминалы и киоски
- **Мобильный телефон**
  - Premium SMS
- **Предоплаченные карты**

КАК ВЫВЕСТИ ДЕНЬГИ? (ВЫВОД СРЕДСТВ ИЗ СИСТЕМЫ)

- **Интернет**
  - Вывод на другую платежную систему
- **Банкинг**
  - Вывод на персональные счета
- **Банкомат**
  - Вывод на платежную карту
- **Отделение банка**
  - Выдача наличных
- **Наличные денежные переводы**
  - В точках работы партнеров системы

Примеры ЭПС:


ЭПС
На базе смарт-карт
На базе интернет- сетей
VISA Cash
тные
Фиатные
PayPal
Нефиатные
QIWI киви
RBK Money
WebMoney
деньги@mail.ru
Яндекс деньги

ВИРТУАЛЬНЫЕ БАНКИ – КТО МОЖЕТ ВЫПУСКАТЬ «СВОИ ДЕНЬГИ»?

- Многопользовательские игры и виртуальные миры – Second Life (Linden $)
- Социальные сети – Facebook Credits
- Порталы и медиа ресурсы – собственные системы расчетов между посетителями и потребителями — Яндекс.Деньги + Яндекс.Маркет, Деньги@Mail.ru
- Любой магазин или поставщик сервисов – подарочные сертификаты и ваучеры
- АЗС и сетевые торговые комплексы – системы лояльности, бонусы и скидки

ЗАЩИТА ЭЛЕКТРОННЫХ ДЕНЕГ

- **Пароли (**контрольный код, PIN-код**)**
- **Файлы ключей(**в платежной системе WebMoney**)**
- **Экранная клавиатура (**в платежной системеEasyPay**)**
- **Контрольная фраза (**в платежной системеEasyPay**)**
- **Блокировка счета**
- **(**экстренная мера**)**

Недостатки электронных денег

- отсутствие устоявшегося правового регулирования, — многие государства ещё не определились в своем однозначном отношении к электронным деньгам;
- несмотря на отличную портативность, электронные деньги нуждаются в специальных инструментах хранения и обращения;
- как и в случае наличных денег, при физическом уничтожении носителя электронных денег, восстановить денежную стоимость владельцу невозможно;
- отсутствие узнаваемости — без специальных электронных устройств нельзя легко и быстро определить владельца, сумму и т. д.;

Мошенничество на финансовом рынке

Мошенничество
«хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотребления доверием»

Финансовое мошенничество

совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Кибермошенничество –

направленные на жертву, умышленные, преступные действия, в реализации которых исполнитель разрабатывает или использует схемы, с применением средств интернета, в интересах нанесения имущественного, финансового вреда, с целью получения материальной выгоды или прибыли, путем ложного представления факта, путем предоставления вводящей в заблуждение информации или путем её сокрытия.

Формы мошенничества и способы минимизации рисков

I. Мошенничество с использованием банковских карт

а) offline:

- банкоматы и терминалы (в т.ч. скимминг)
- оплата в магазинах или ресторанах

Способы минимизации рисков

- пользоваться только банкоматами, установленными в безопасных местах
- внимательно осматривать банкомат, перед его использованием
- закрывать клавиатуру при вводе пин-кода
- оформить услугу SMS-оповещения о проведенных операциях по карте
- не давать согласие на получение карты по почте и ее активации по телефону
- не хранить пин-код вместе с картой
- не сообщать по мобильным или стационарным телефонам реквизиты карты и ее пин-код
- определить лимит суточного снятия наличных по карте
- блокировать карту немедленно в случае утери/хищения

Терминология

Скимминг* — установка на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковской карты и вводимый пин-код) для последующего хищения денежных средств со счета банковской карты.

*от англ. skim - снимать сливки

Формы мошенничества и способы минимизации рисков

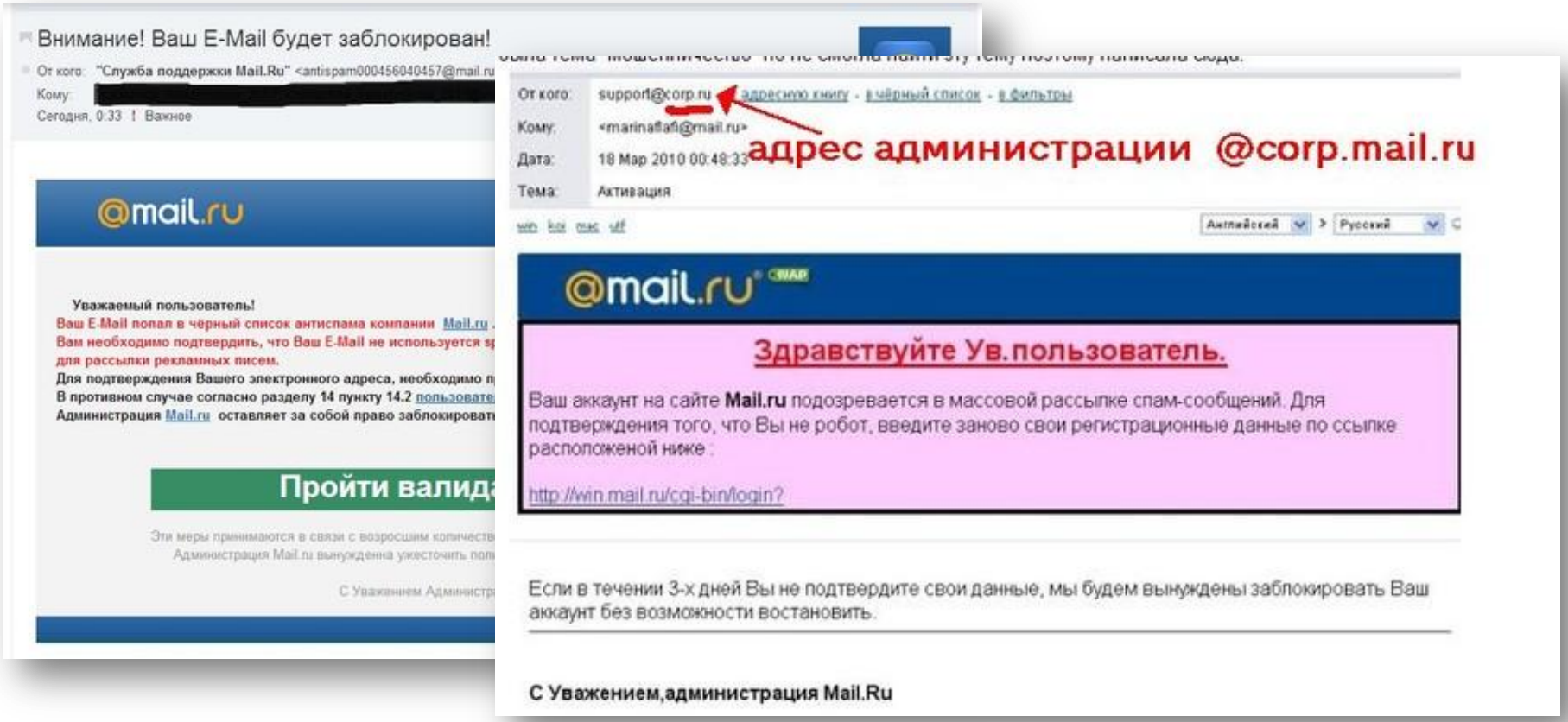
I. Мошенничество с использованием банковских карт	Способы минимизации рисков
б) online: • интернет-мошенничества	• установить программы защиты и обеспечения безопасности компьютера в Интернете • проводить финансовые операции только с защищенных веб-сайтов • не сообщать пароль доступа к своему счету через интернет • использовать надежные пароли • по окончании работы выходить из учетной записи • не отвечать на электронные сообщения с запросом на изменение параметров защиты • использовать разные инструменты для разных видов расчетов

Формы мошенничества

III. Кибермошенничество

Терминология

Фишинг (англ. phishing) – это технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт, посредством спамерской рассылки или почтовых червей.



Формы мошенничества и способы минимизации рисков

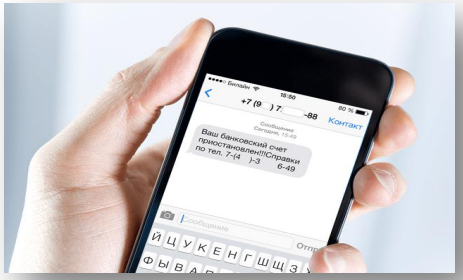
II. Кибермошенничество

Фишинг:

- а) почтовый
- б) онлайновый
- в) комбинированный

Способы минимизации рисков

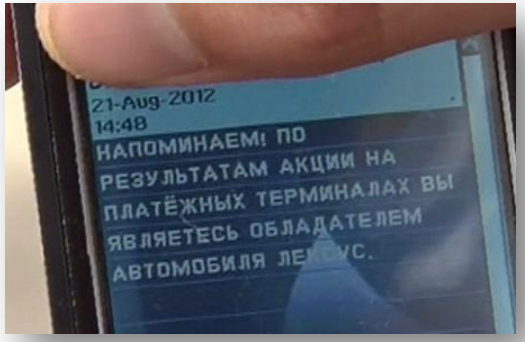
- проявлять осторожность
- застраховать карту от риска мошенничества
- использовать разные инструменты для разных видов расчетов
- использовать метод многофакторной аутентификации



Терминология

Вишинг (англ. vishing) – это технология интернет-мошенничества, заключающаяся в использовании автонабирателей и возможностей интернет-телефонии для кражи личных конфиденциальных данных, таких как пароли доступа, номера банковских и идентификационных карт и т.д.

Смишинг – это вид мошенничества, при котором пользователь получает СМС-сообщение, в котором с виду надежный отправитель просит указать какую-либо ценную персональную информацию (например, пароль или данные кредитной карты). Смишинг представляет собой подобие фишинга, при котором мошенниками с той же целью рассылают электронные письма.



Формы мошенничества и способы минимизации рисков

II. Кибермошенничество

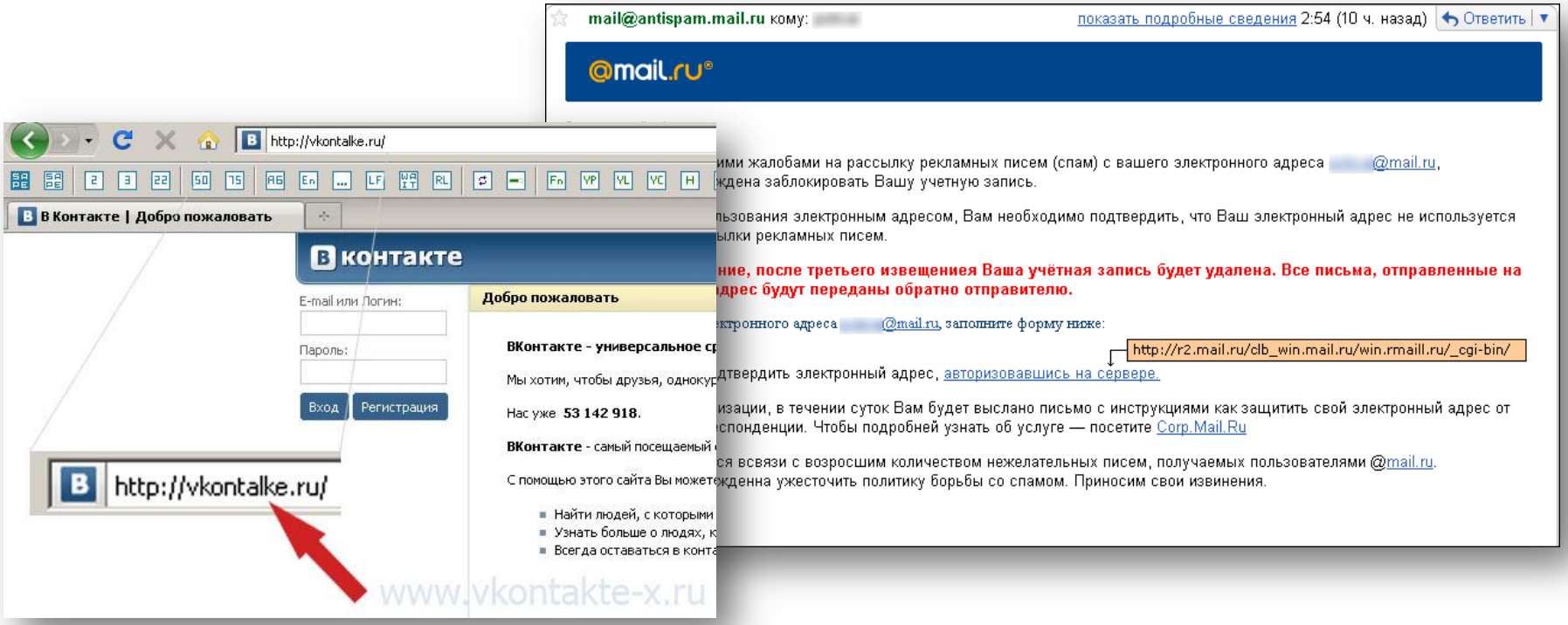
- Вишинг
- Смишинг

Способы минимизации рисков

- внимательно изучить правила безопасного использования банковской карты
- не сообщать никому, в том числе сотруднику банка, ваши персональные данные и данные банковской карты;
- при возникновении факта мошенничества обратиться в ваше отделение банка
- в случае необходимости заблокировать карту
- не звонить по предложенному в смс номеру телефона по вопросам безопасности вашей карты

Терминология

Фарминг (англ. pharming) – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации.



Формы мошенничества и способы минимизации рисков

II. Кибермошенничество	Способы минимизации рисков
Фарминг	• установка антивирусной программы • установка обновлений от производителей ПО и поставщика услуг Интернета. • проверка URL • проверка изменения адреса http на https при переходе на страницу оплаты

Терминология

«Нигерийские письма» (англ. «Nigerianscam») – электронное письмо с просьбой о помощи в переводе крупной денежной суммы, из которой 20-30% должно получить лицо, предоставляющее счет. При этом получателю необходимо срочно 6-10 тысяч долларов США отправить по системе электронных платежей по требованию адвоката.

Как разновидность используется рассылка о выгодном капиталовложении или устройстве на высокооплачиваемую работу, получении наследства или иных способах быстрого обогащения при условии совершения предварительных платежей.

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
«Нигерийские письма»	• установить антиспамерские программы • критически относиться к предложениям получения быстрого и необоснованного дохода • получить консультацию экспертов в области финансового мошенничества • проявлять осмотрительность при принятии быстрых финансовых решений

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

- Интернет-аукцион
- Электронная торговля
- Скандинавский аукцион
- Семь кошельков
- С помощью платежной системы

Способы минимизации рисков

- пользуйтесь проверенными мировыми и российскими торговыми площадками
- заключайте сделку только через выбранную площадку
- требуйте максимально полной информации о продавце дешевого товара
- по возможности оплачивайте товар по факту его получения

Мошенничество с PayPal*

1. Вы разместили объявление о продаже
2. Мошенник высылает Вам письмо с предложением купить товар, иногда за большую цену и не для себя
3. Вы просите перевести деньги
4. Мошенник просит вас указать адрес, зарегистрированный в PayPal и говорит что выслал деньги туда, но они появятся на счёте в PayPal, когда вы введете номер почтового отправления
5. К вам приходит письмо, похожее на PayPal
6. Вы отправляете товар и вводите номер отправления в указанную в письме страницу

Товара у вас нет. Претензии выставлять некому

*PayPal - крупнейшая дебетовая электронная платёжная система
Аналоги в РФ: Яндекс.Деньги, WebMoney

Терминология

Кликфрод (от англ. click fraud) — один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении. Может осуществляться с помощью автоматизированных скриптов или программ, имитирующих клик пользователя по рекламным объявлениям Pay per click.

Кликджекинг (от анг. clickjacking) механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу.

Виды кликфрода

технические клики

клики рекламодателей

клики конкурентов

клики со стороны недобросовестных веб-мастеров

Терминология

PAMM-счета (от англ. Percent Allocation Management Module – модуль управления процентным распределением) – специфичный механизм функционирования торгового счёта, технически упрощающий процесс передачи средств на торговом счёте в доверительное управление выбранному доверенному управляющему для проведения операций на финансовых рынках.

Формы мошенничества и способы минимизации рисков

II. Кибермошенничество	Способы минимизации рисков
Хайп	• провести «тестовый режим» участия в хайп-проекте • анализировать информацию сайтов-мониторингов и форумов, освещающих состояние дел по интересующему вас хайп-проекту • распределять денежные средства между несколькими хайп-проектами • не инвестировать заемные средства • не инвестировать «последние деньги»

Другие виды финансового мошенничества

Финансовое мошенничество	Способы минимизации рисков
- обмен валюты	- совершать валютно-обменные операции в банках; - минимизировать данные операции в обменных пунктах; - быть внимательным, так как курс может быть указан без учета комиссии, либо выгодным он является исключительно при обмене очень больших сумм; - всегда пересчитывать денежную сумму.
- нелегальные кредиты	- изучить официальную информацию о компании (реквизиты, юридический и фактический адрес) ; - проверить наличие информации о финансовой компании на сайте надзорного органа – ЦБ РФ; - посмотреть отзывы о компании в независимых блогах и социальных сетях.

Другие виды финансового мошенничества

брачные аферы

нелегальные азартные игры

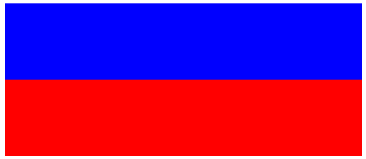
раздолжнители

махинации с арендой/покупкой недвижимости или автомобилей

использование чужих паспортов для сомнительных сделок

Основные общие признаки указывающие на риски финансового мошенничества

- ✓ вознаграждение существенно превышает деловую практику по данному типу сделок;
- ✓ использование технологий «социальной инженерии» и манипулирование такими интересами как жадность, желание быстро разбогатеть, зависть;
- ✓ предложение решить все финансовые проблемы в короткий срок;
- ✓ необходимость первоначальных выплат;
- ✓ анонимность контрагента;
- ✓ необходимость мгновенного принятия сложного финансового решения;
- ✓ несоответствие складывающейся ситуации стандартной схеме;
- ✓ наличие указания на эксклюзивный, кастомизированный характер предложения.



Современный опыт законодательной борьбы с финансовым мошенничеством

- Статья 159.1 УК РФ Мошенничество в сфере кредитования
- Статья 159.2 УК РФ Мошенничество при получении выплат
- Статья 159.3 УК РФ Мошенничество с использованием платежных карт
- Статья 159.5 УК РФ Мошенничество в сфере страхования
- Статья 159.6 УК РФ Мошенничество в сфере компьютерной информации

Если вы стали жертвой мошенников

Необходимо немедленно обратиться в полицию.

Для правоохранителей совсем неважно было ли совершенно преступление на улице или в интернете, они будут вынуждены принять меры.